Leibniz Supercomputing Centre

of the Bavarian Academy of Sciences and Humanities

The DigiMed Bayern Secure Cloud

Secure at Heart: How We Built a Collaborative Medical Research Cloud Platform Around Confidential Computing Technologies

December 5th 2023 | DigiMed Symposium | Florent Dufour, Dr. Naweiluo Zhou

Work package 6: IT Conception and Infrastructure

One of DigiMed Bayern's key strengths is the innovative design and implementation of a centralized digital platform, which not only guarantees secure, data protection-compliant data access, but also analytical tools, algorithm-based analysis including machine learning, and knowledge management systems. The use of AI in these areas has been established for a relatively long time. It extends in the free text area (text mining) from the recognition and assignment of words and word groups in ontologies to syntactic and semantic analysis and subsequent structuring of information in databases. In the field of image recognition, for example, histological microscopic patterns can be recognized and quantified. As a special application within DigiMed Bayern, the establishment and use of a high-throughput process is envisaged in WP5.2, for example, in which lasers for microdissociation of the plaques originating from WP2 are then controlled on the basis of evaluated image data. The prepared plaque areas are then to be examined by proteomics methods, and thus contribute to the causal connection with the clinical progression of stroke patients through to new therapeutic approaches.

The collection, analysis and evaluation of medical big data are closely supported by the statistical expertise of the partners. The goal is to establish a largely comprehensive and cooperative digital infrastructure, which is contemporary and feasible at the same time.

The collection, processing, merging and integrative analysis of large sets of different data, as aimed for in DigiMed Bayern, requires the use of various IT technologies. The aim is to integrate these technologies and create an infrastructure that connects the IT resources available at the partner sites involved, and thereby enables efficient sharing of the data and tools required for the project. The requirements for this infrastructure are also partially described in WPs 1 to 5. In addition to the infrastructure, it is also required to build up the DigiMed partners' competence to use them correctly and purposefully, and thus profitably for the medical benefit.

There will be close horizontal cooperation between the institutions involved in DigiMed Bayern with regard to data types, volumes, protection, integration and evaluation. At the same time, the interdisciplinary setting of the team, such as computer

Prof. Dr. med. Heribert Schunkert

Wissenschaftlicher Leiter DigiMed Bayern, Direktor der Klinik für Herz- und Kreislauferkrankungen am Deutschen Herzzentrum München

+49 (0) 89 / 1218-4073
wildgruber@dhm.mhn.de

Prof. Dr. Annette Peters

The primary task in WPs 1 to 5 is to record the existing hardware and software infrastructure, of the data and use cases, in order to then jointly develop a solid concept that also includes the LRZ infrastructure in the implementation. This also creates a connection to the computer capacity that is required to implement the data analysis in WPs 1 to 5.

WP6.1 Analysis of the existing infrastructure / conception of the integrative IT infrastructure

First, the status quo of the existing IT infrastructures of the partners involved is evaluated. In order to arrive at an early assessment of the integrability into a higher-level infrastructure, all important questions regarding the current status of IT equipment, data management requirements and the requirements of the scientists for an integrative infrastructure are identified and categorized in the first six months. A questionnaire is filled in during interviews with the IT specialists from all partner institutions. These surveys are carried out in close cooperation with WP7 under the requirements of ethics and data protection. A comprehensive workshop at the beginning of the project lays the foundation. The results serve for the subsequent conception of the infrastructure. This takes into account both the local inventory of resources, data and tools, as well as infrastructures that are available internationally at other locations or with other cooperation partners.
For the design of the required infrastructure, particular attention is paid to the requirements for analysis and knowledge management software from WP6.3. Conversely, the analysis results from WP6.1 flow into WP6.3, especially with regard to security, data protection, scalability, usability, compatibility of hardware architectures, interfaces, data formats, etc. The process of defining requirements and selection is coordinated and controlled by the LRZ.

The documented results of the conception phase are used for the detailed planning of the construction of the infrastructure in the second project phase. A continuous training program developed by WP6.2 familiarizes the project partners with the infrastructure, and jointly identifies suggestions for improvement and further developments for further integration. After construction and operation, a goal is also the transfer of the infrastructure to clinical or clinic-related operation in year 5, and the public-available documentation as an exemplary, scalable and transferable infrastructure for P4 medicine with omics data.

WP6.2 Development of the pilot infrastructure, planning and coordination of the data exchange, provision of computing capacity

In order to efficiently utilize the conception phase, and to allow realistic experiences to flow into the conception continuously despite the complex analysis of requirements and status quo, the first parts of the integrative infrastructure with a focus on "low hanging fruits" are being developed in parallel. IT resources are set up in such a way that pilot applications on the first infrastructure components can be tested and used as quickly as possible. Such a component will be, for example, the database, which centrally stores the biochemical and molecular genetic data and the treatment of FH patients, or public-available gene and protein databases with phenotypical associations and ontologies. Until all questions relating to data protection regulations are clarified, only non-critical data will be used for the testing phase. In addition to data storage, data transfer between the institutions and the central data management facilities is also made possible. The need for scaling of data transfer infrastructures to defined, high volumes of data is taken into account early in the operating phase.

Prof. Dr. Thomas Meitinger

Leitung Institut für Humangenetik, Klinikum rechts der Isar, Technische Universität München

+49 (0) 89 / 4140-6381
sekretariat.ihg@mri.tum.de

Prof. Dr. Matthias Mann

Director Department of Proteomics and Signal Transduction, Max-Planck-Institute of Biochemistry

+49 (0) 89 / 8578-2557
mmann@biochem.mpg.de

Prof. Dr. Dieter Kranzlmüller

Vorsitzender des Direktoriums des LRZ

+49 (0) 89 / 35831-8700
lrzpost@lrz.de

the second project phase. A continuous training program developed by WP6.2 familiarizes the project partners with the infrastructure, and jointly identifies suggestions for improvement and further developments for further integration. After construction and operation, a goal is also the transfer of the infrastructure to clinical or clinic-related operation in year 5, and the public-available documentation as an exemplary, scalable and transferable infrastructure for P4 medicine with omics data.

WP6.2 Development of the pilot infrastructure, planning and coordination of the data exchange, provision of computing capacity

In order to efficiently utilize the conception phase, and to allow realistic experiences to flow into the conception continuously despite the complex analysis of requirements and status quo, the first parts of the integrative infrastructure with a focus on "low hanging fruits" are being developed in parallel. IT resources are set up in such a way that pilot applications on the first infrastructure components can be tested and used as quickly as possible. Such a component will be, for example, the database, which centrally stores the biochemical and molecular genetic data and the treatment of FH patients, or public-available gene and protein databases with phenotypical associations and ontologies. Until all questions relating to data protection regulations are clarified, only non-critical data will be used for the testing phase. In addition to data storage, data transfer between the institutions and the central data management facilities is also made possible. The need for scaling of data transfer infrastructures to defined, high volumes of data is taken into account early in the operating phase.

In addition to the transfer and management of the data, their processing is an essential part of the IT infrastructure. For this purpose, analysis software must be partially installed on central hardware components, which can provide the computing capacity required for the corresponding calculations. For HPC systems, such as those used for large simulations or analysis, a separate application is required that demonstrates the scientific and technical expertise necessary to use the systems. The LRZ supports the responsible scientists in preparing these applications. In addition, tests of the software are carried out on the infrastructure, the results of which flow directly into its design at WP6.1.
Following a process of continuous integration, this pilot infrastructure will be gradually expanded and improved. In this way, the growing possibilities can be tested for suitability by pilot users, and any deficits can be immediately incorporated into the further concept. At the end of the first phase, the knowledge gained from setting up and testing the pilot infrastructure is gathered and integrated into the documentation for WP6.1. This serves to decide on the continuation of pilot components in real operation, or the redesign of sub-areas that may not be sufficiently viable.

In the second phase, the concept of WP6.1 is implemented iteratively and operated for use by the scientists from WPs 1 to 5. At the same time, the transfer to clinical or clinic-related operations is being prepared independently of DigiMed Bayern, which is planned to take place in year 5.

WP6.3 Analysis, conception and implementation of software solutions for the integrated omics platform and the expert system for digital medicine

The data protection-compliant integration of existing as well as prospective and retrospective data is the basis for further analysis. For this purpose, a comprehensive IT core infrastructure is to be created, which supports the acquisition, processing, integration and analysis of big data. Public data used in the project should be in compatible formats that can be evaluated digitally and integrative, and be made accessible and integrated. At the command line or graphical user interface level, it should

Prof. Dr. Dieter Kranzlmüller

Vorsitzender des Direktoriums des LRZ

+49 (0) 89 / 35831-8700
lrzpost@lrz.de

Prof. Dr. Ulrich M. Gassner

Professor für Öffentliches Recht, Universität Augsburg

+49 (0) 821 / 598-4600
ulrich.gassner@jura.uni-augsburg.de

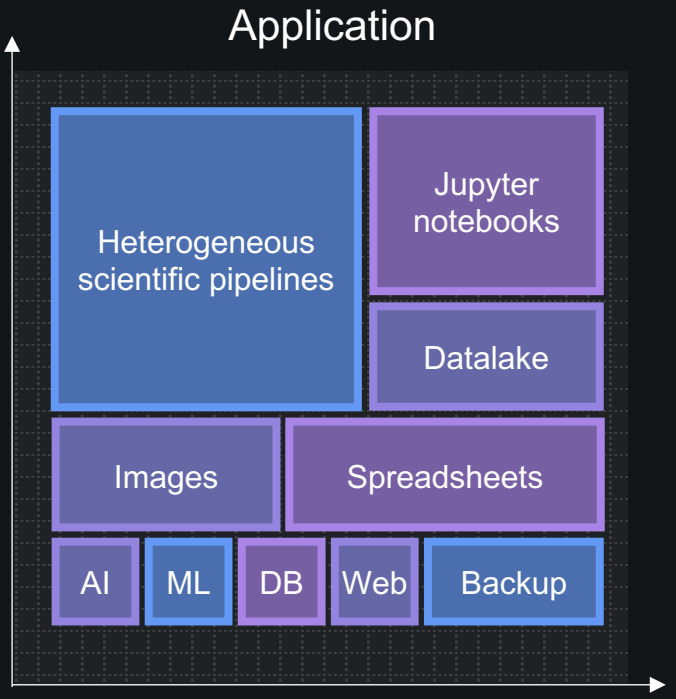
Dr. Jens Wiehler

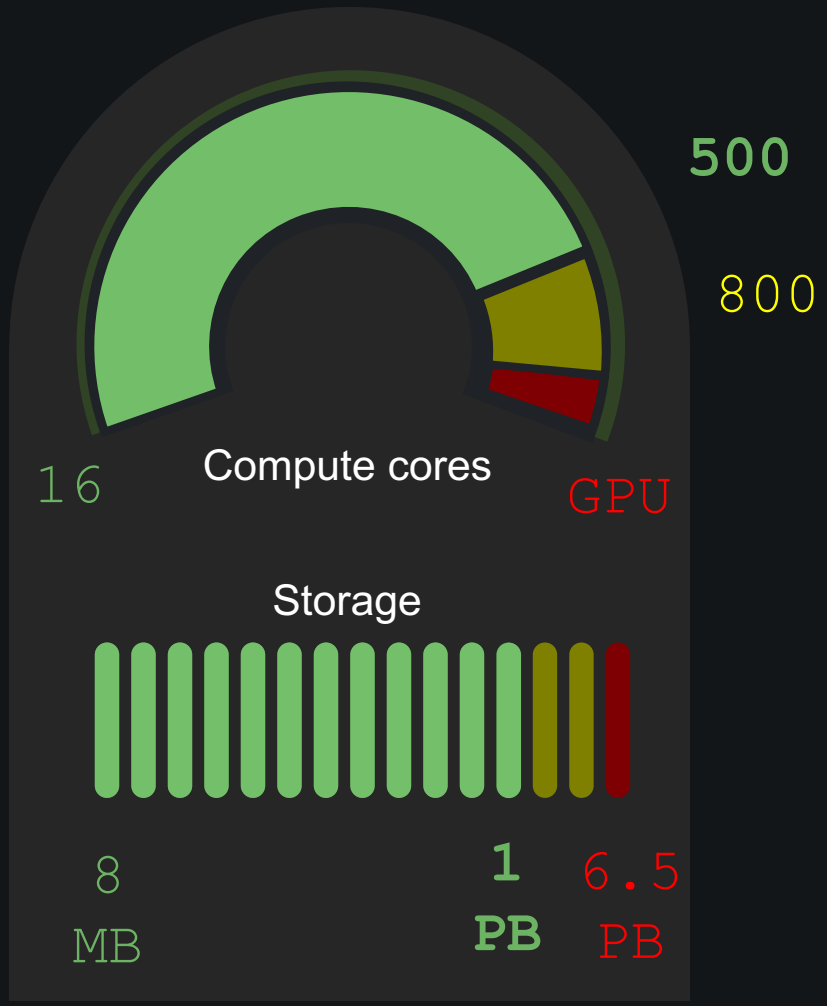
Digital Health Lead, Managing Director DigiMed Bayern

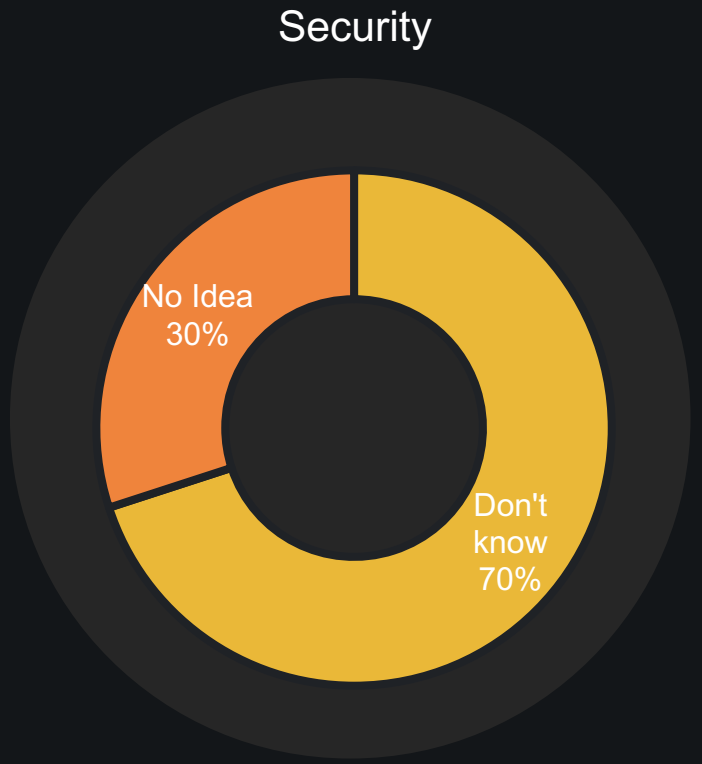
+49 (0) 89 / 89 96 79-36
wiehler@bio-m.org

1- **Planning** for the DigiMed Bayern Secure Cloud

Survey of Users Requirements

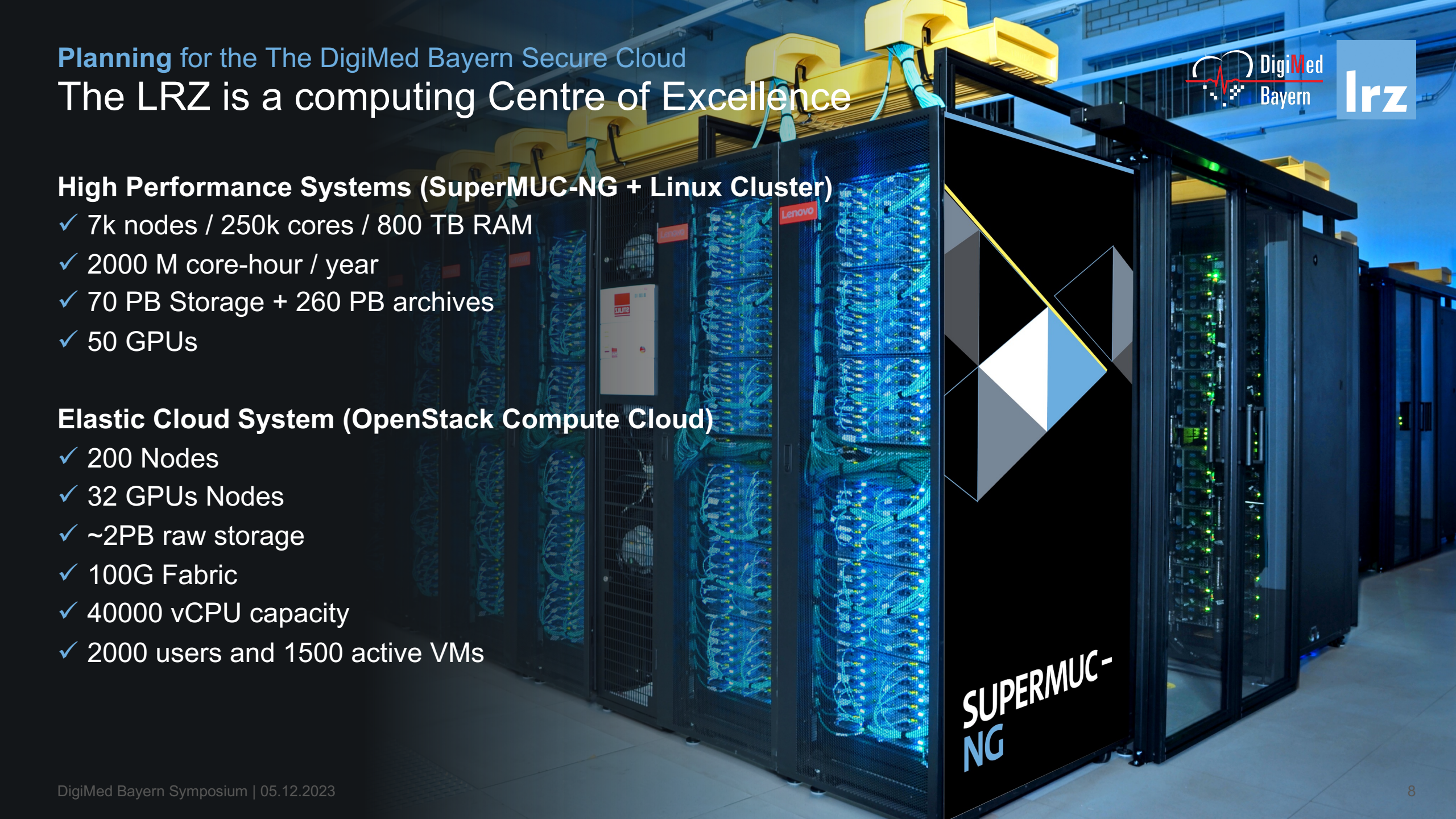






Planning for the The DigiMed Bayern Secure Cloud

The LRZ is a computing Centre of Excellence



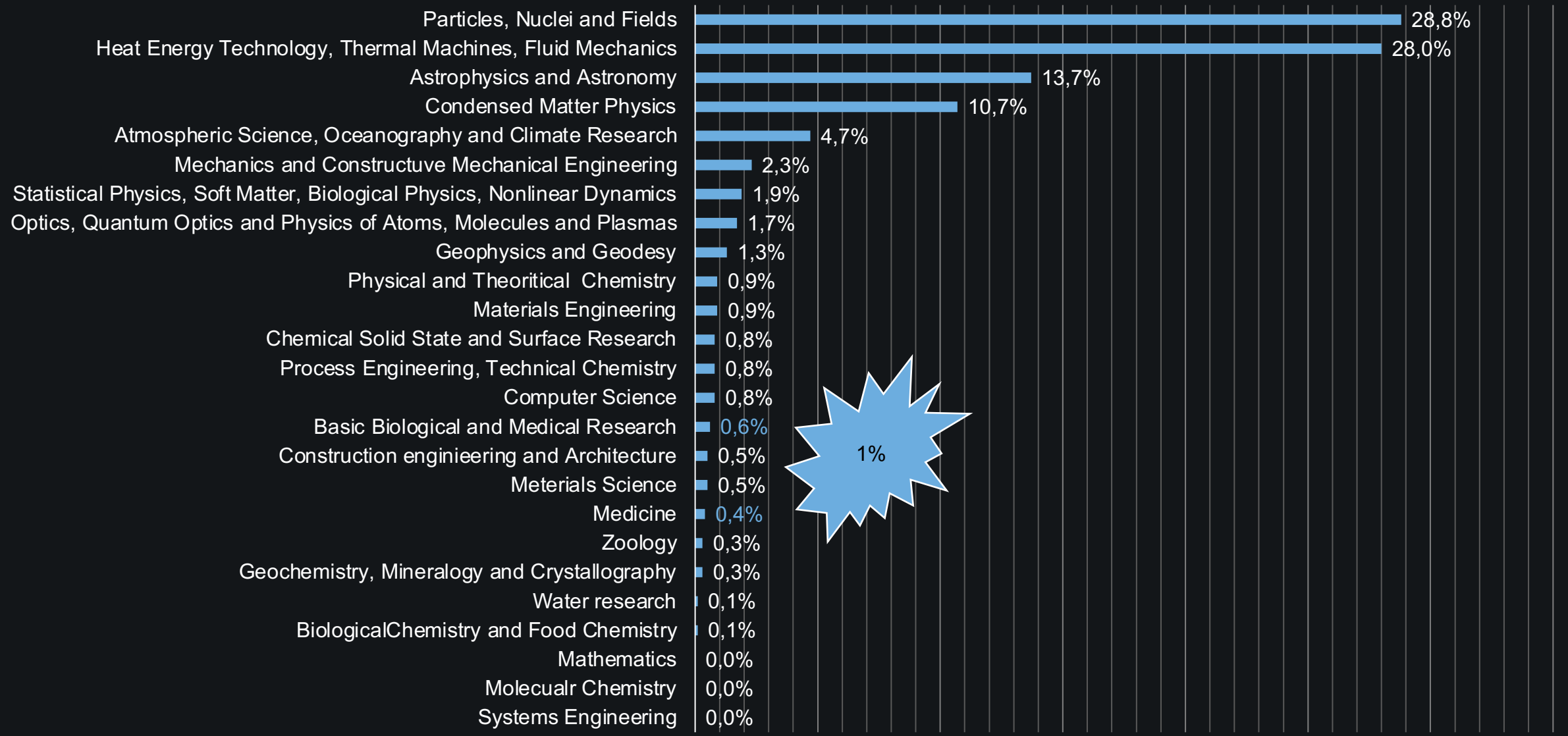
High Performance Systems (SuperMUC-NG + Linux Cluster)

- ✓ 7k nodes / 250k cores / 800 TB RAM
- ✓ 2000 M core-hour / year
- ✓ 70 PB Storage + 260 PB archives
- ✓ 50 GPUs

Elastic Cloud System (OpenStack Compute Cloud)

- ✓ 200 Nodes
- ✓ 32 GPUs Nodes
- ✓ ~2PB raw storage
- ✓ 100G Fabric
- ✓ 40000 vCPU capacity
- ✓ 2000 users and 1500 active VMs

Biomedical Research is not conducted on LRZ Systems



2 - **Architecting** the DigiMed Bayern Secure Cloud

DigiMed enabled an Integral Collaboration

IT Expertise **Legal Expertise**

DigiMed enabled an Integral Collaboration

IT Expertise **Legal Expertise**

Security
- ✓ Comprehensive security concept
- ✓ Threat model and mitigation
- ✓ Physical security measures
- ✓ End-to-end data encryption

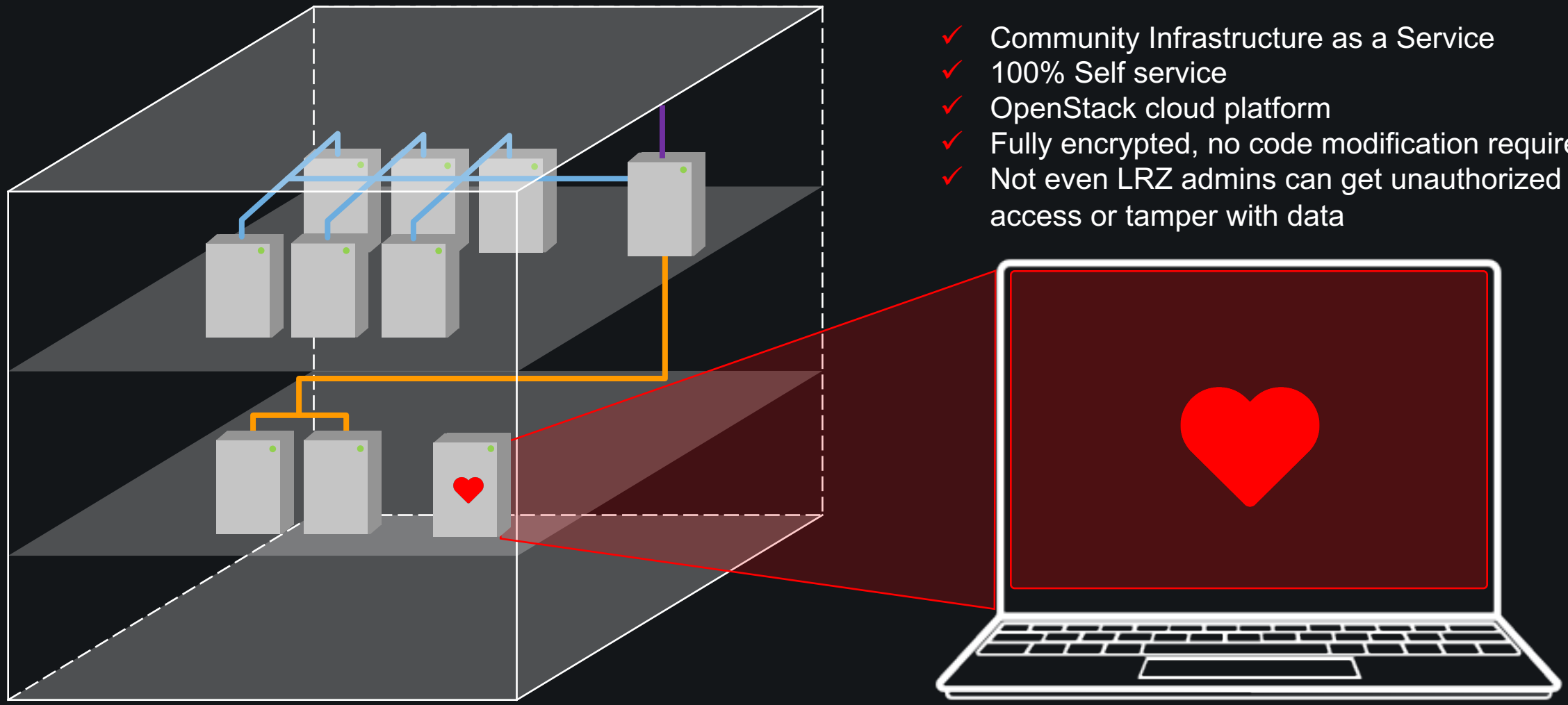
Privacy
- ✓ Pseudonymisation of data
- ✓ Logical and cryptographic separation of tenants

Sustainability
- ✓ Scalability and future proofing
- ✓ GAIA-X federation Support

- ✓ Gesetz: Change in the Art. 27 Abs. 4 S. 6 of the Bayerischen Krankenhausgesetzes („BayKrG“)
- ✓ AVV: Auftragsverarbeitungs-Vertrag
- ✓ TOMs: Technical and Organisational measures
- ✓ DSFA: Data Protection Impact Assessment
- ✓ Usage regulation and user security training

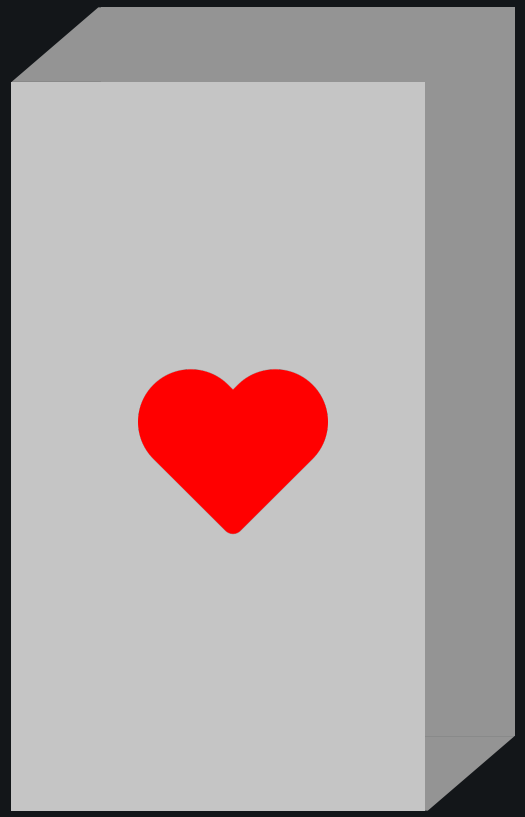
Co-design with the Data Protection Officier
150 Documents in the Dokumentenlandkarte Datenschutz

The DigiMed Secure Cloud is Standalone



- ✓ Community Infrastructure as a Service
- ✓ 100% Self service
- ✓ OpenStack cloud platform
- ✓ Fully encrypted, no code modification required
- ✓ Not even LRZ admins can get unauthorized access or tamper with data

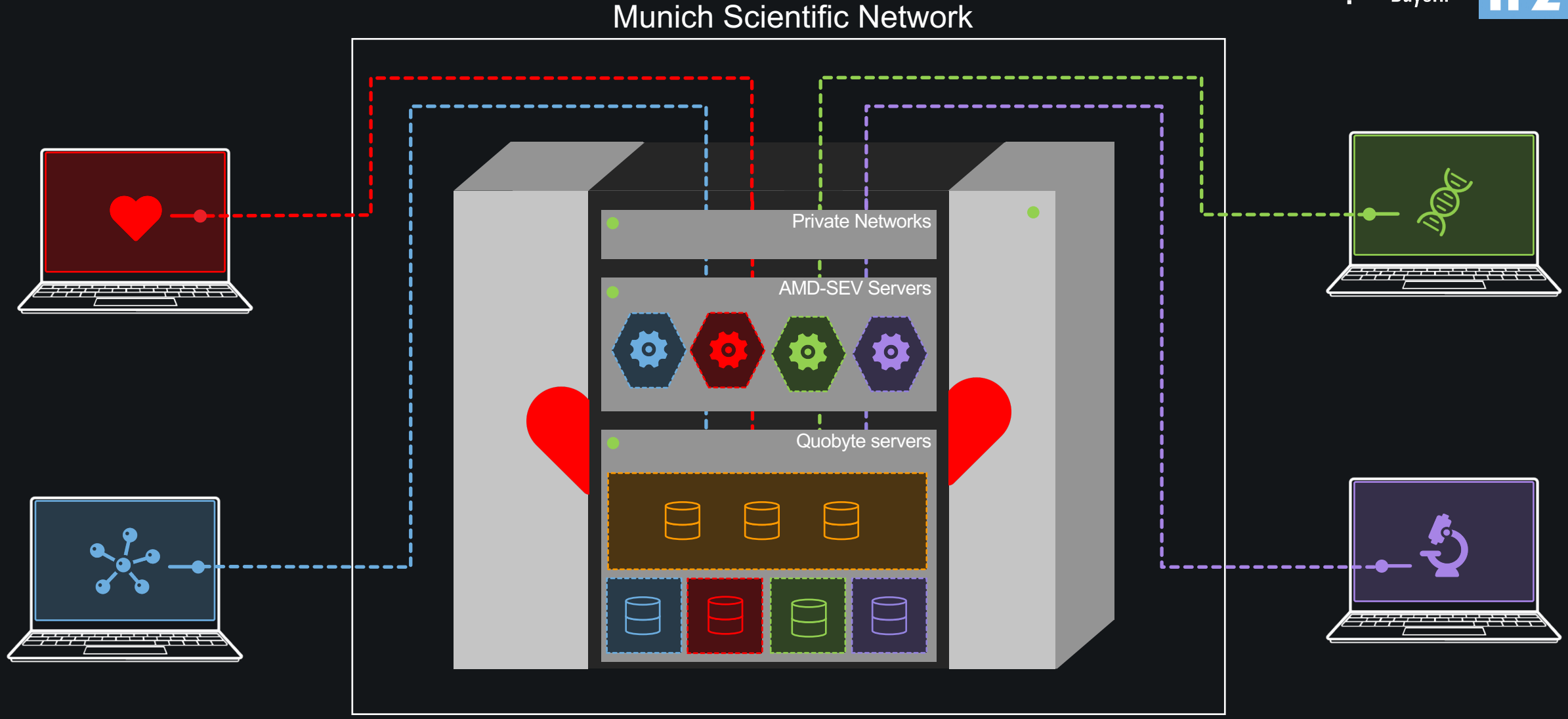
The DigiMed Secure Cloud is Standalone



dotted line = encrypted

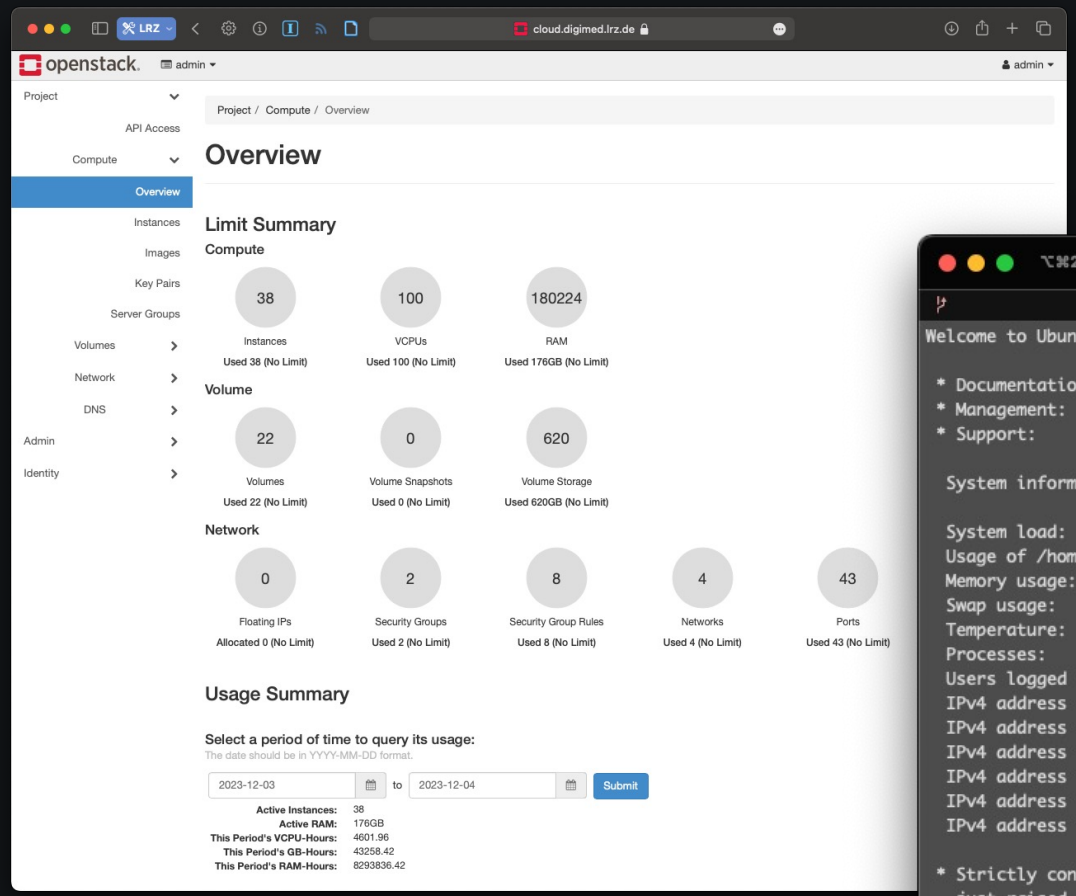
DigiMed Bayern

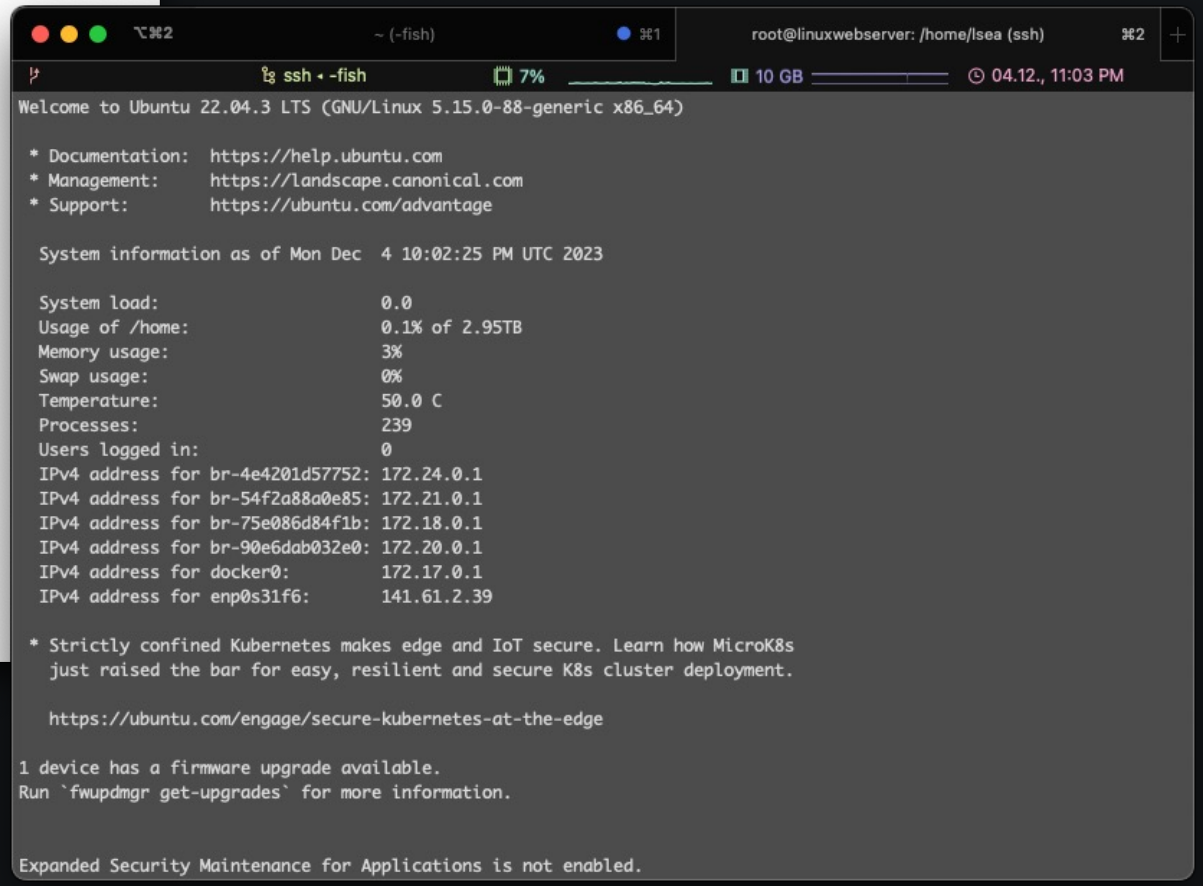
lrz



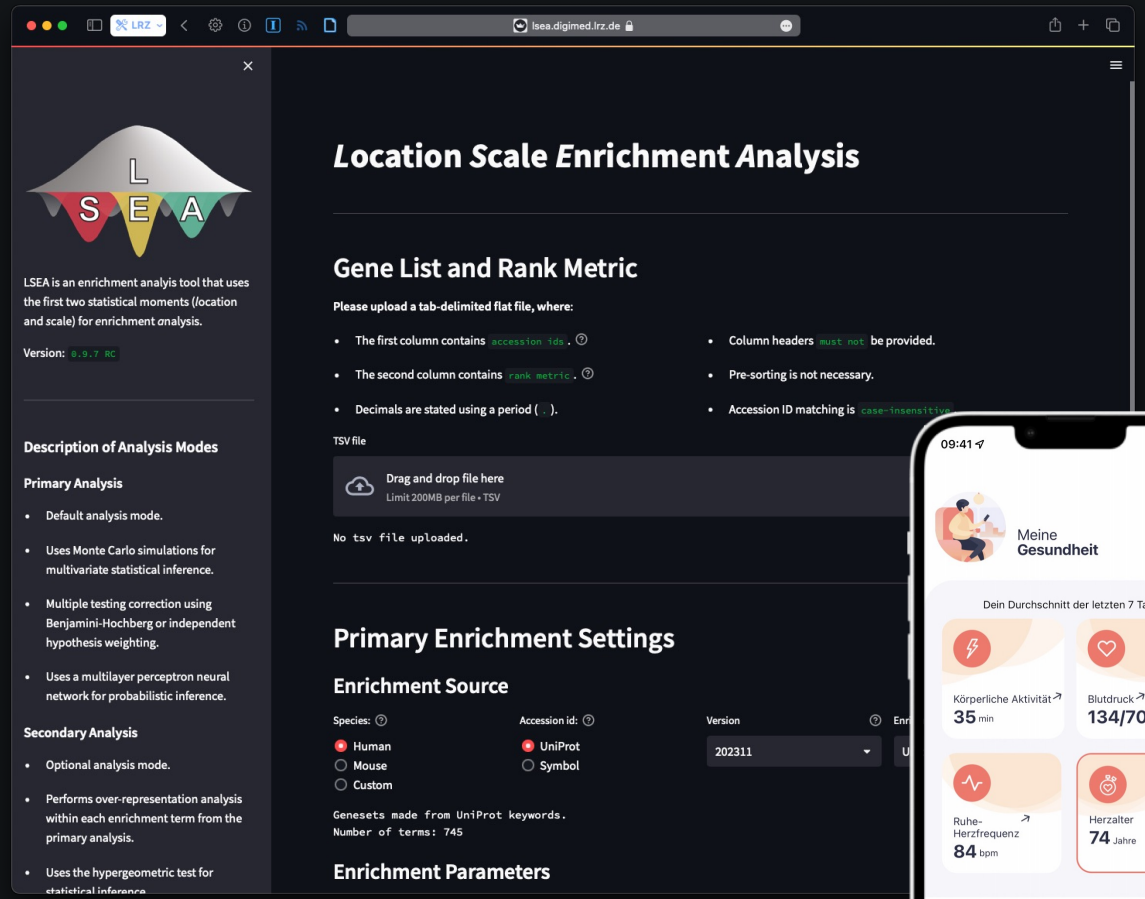
Data is encrypted in all states: at rest, in flight, in use.

The DigiMed Secure Cloud is being tested





Some DigiMed Bayern Usecases are being migrated



3 - Scientific output of WP6

Publications

- Published:

1. N. Zhou, F. Dufour, V. Bode, P. Zinterhof, N. J. Hammer, and D. Kranzlmller, “Towards Confidential Computing: A Secure Cloud Architecture for Big Data Analytics and AI,” in *IEEE International Conference on Cloud Computing (IEEE CLOUD)*, (Chicago, Illinois, USA), 2023.
2. F. Dufour, N. Zhou, V. Bode, P. Zinterhof, N. J. Hammer, D. Kranzlmüller, “Towards Confidential Computing: A Cloud Architecture for Big Data Analytics and AI in Biomedical Research (poster),” in ISC, Hamburg, Germany, May 2023.

- Talk:

1. F: Dufour, “Towards the Medicine of the Future in Bavaria and Germany, One Heartbeat at the Time With Confidential Computing,” in Open Confidential Computing Conference (OC3), Online, 2023.

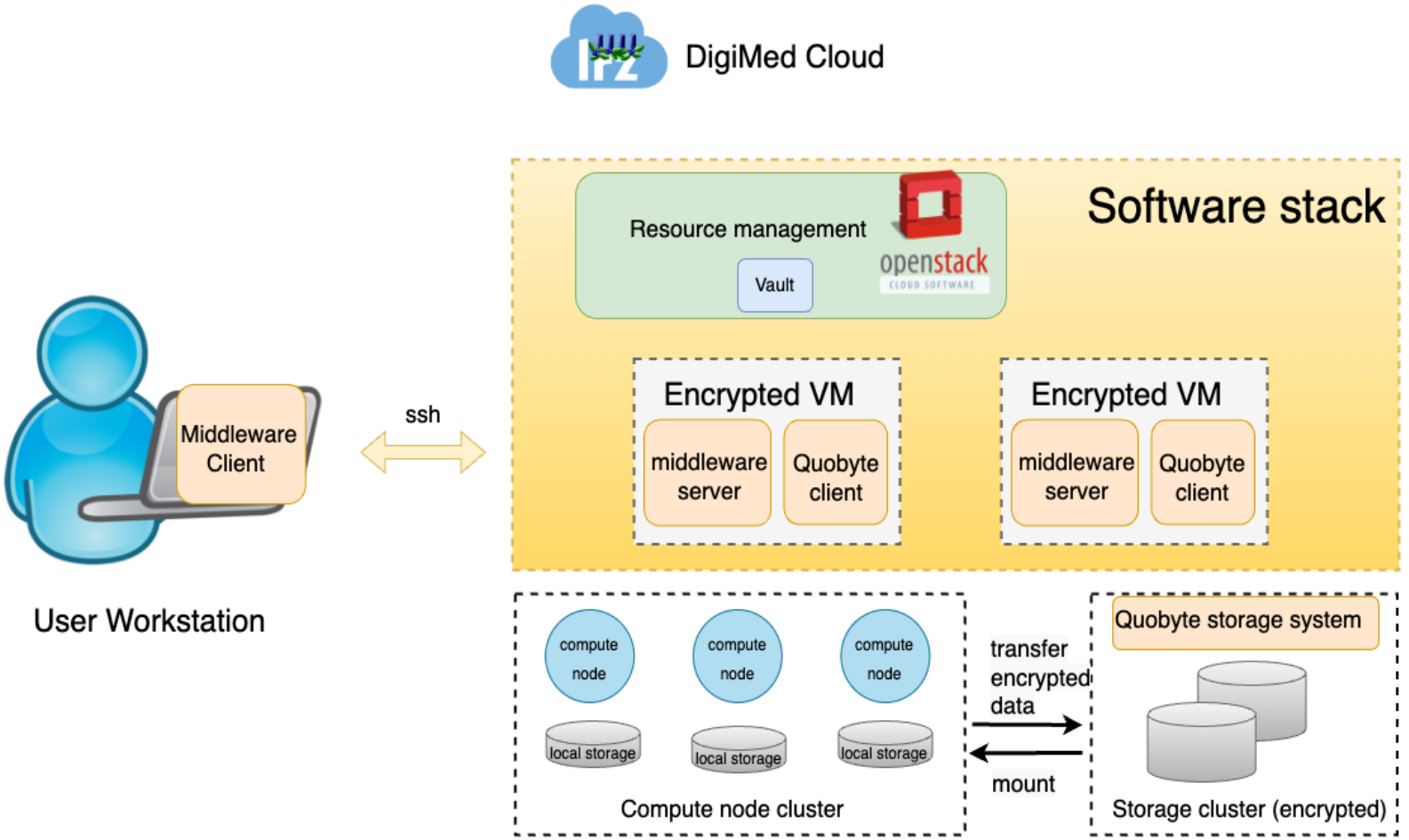
- Planned:

Extended version for tier1 scientific journal or research conference, 2024

Secure Your Workflow with LRZ DigiMed Cloud

Main components of the Cloud

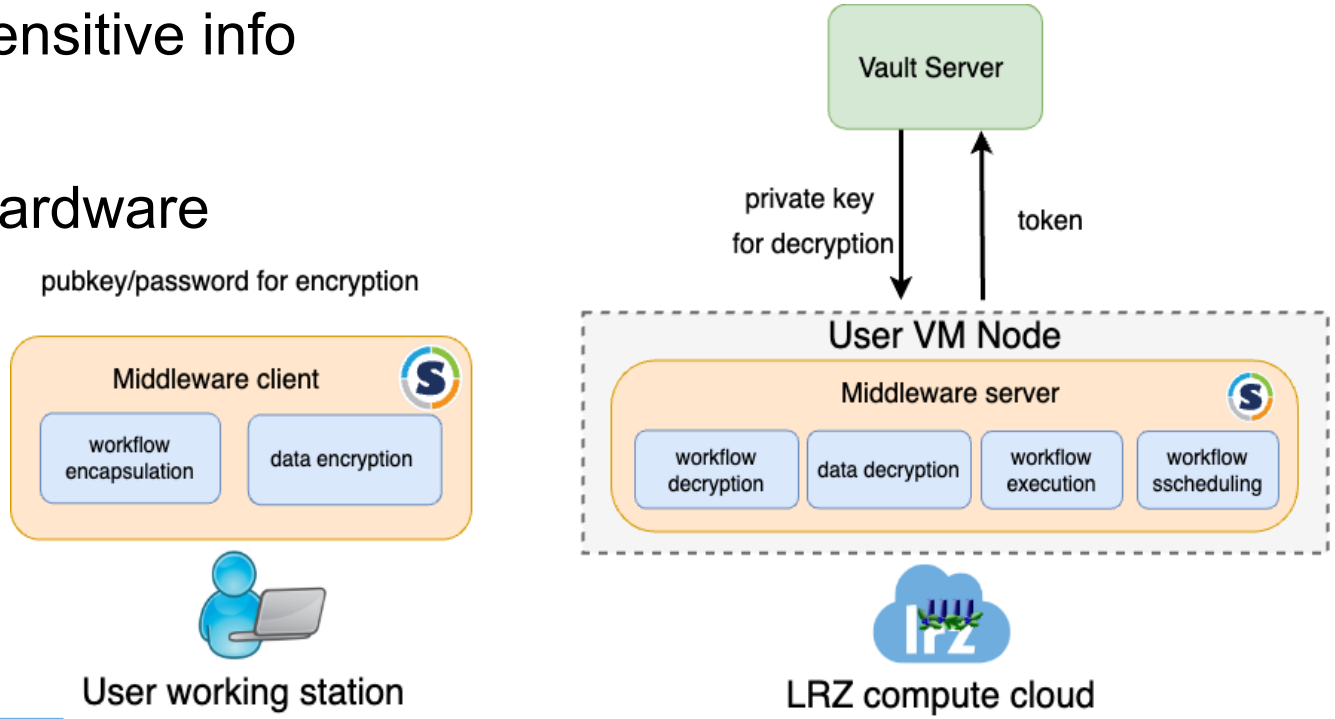
- Storage node
- Compute node, control node
- Software stack



Secure Your Workflow with LRZ middleware

Purpose:

- Your workflow and data includes sensitive info
- Safely transfer over network
- More portable, independent from hardware
- Prevent attacks from VM level



Your entire workflow and data are encrypted!

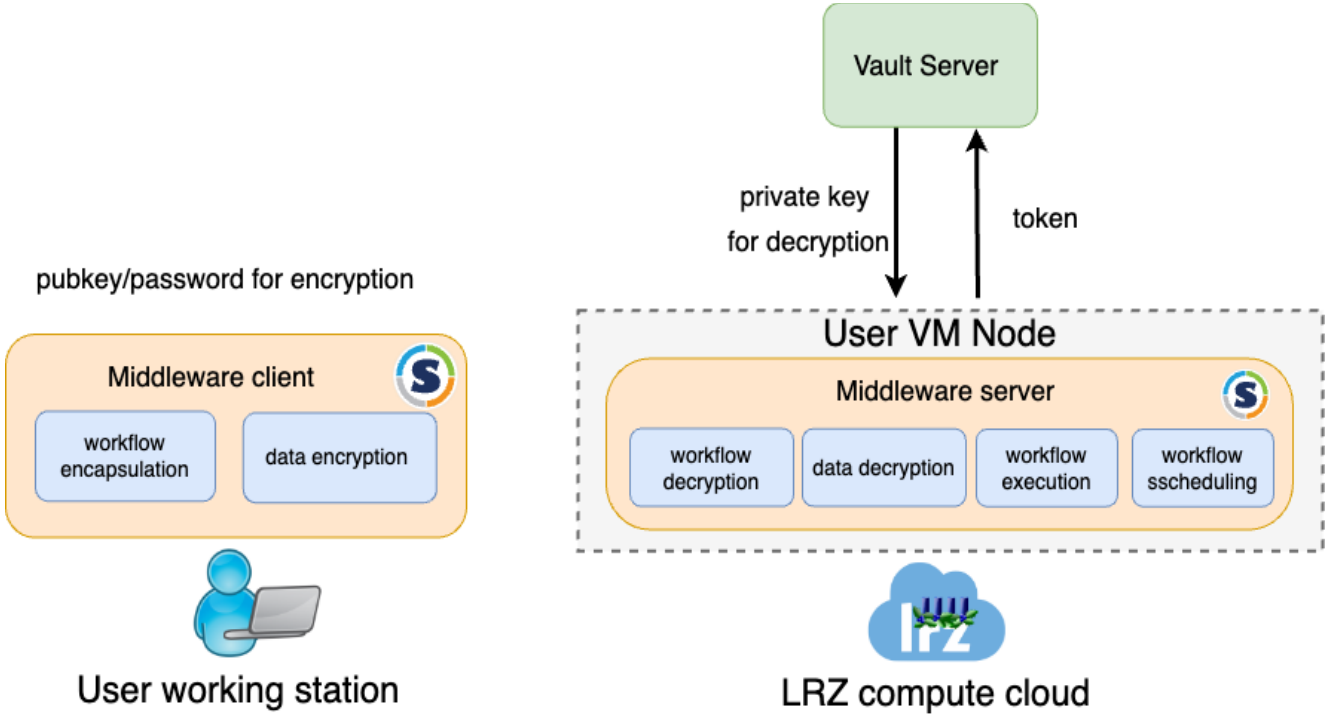
the main components of LRZ middleware

* N. Zhou, F. Dufour, V. Bode, P. Zinterhof, N. J. Hammer, and D. Kranzlmller, “Towards Confidential Computing: A Secure Cloud Architecture for Big Data Analytics and AI,” in *IEEE International Conference on Cloud Computing (IEEE CLOUD)*, (Chicago, Illinois, USA), 2023.

Secure Your Workflow with LRZ middleware

Main functionalities

- Pack your code inside encrypted **workflow container**
- Pack your data (if large size, e.g. 200GB) into an encrypted **data container**
- Schedule and execute the workflow

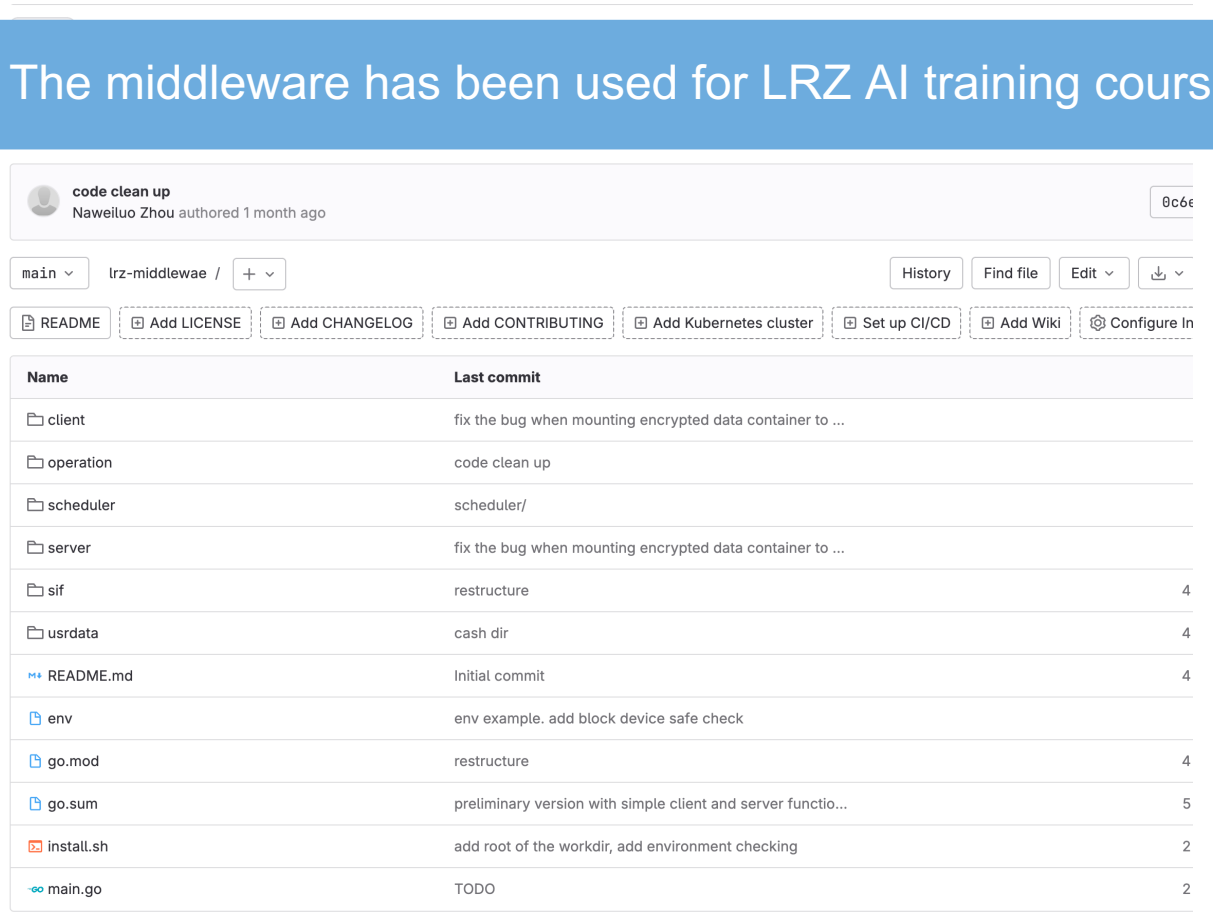


the main components of LRZ middleware

Secure Your Workflow with LRZ middleware

- Available on LRZ GitLab
- More features to come

The middleware has been used for LRZ AI training courses



Acknowledgment

LRZ

- ♡ Prof. Dieter Kranzlmüller
- ♡ Dr. Anton Frank*
- ♡ Dr. Nicolay Hammer
- ♡ Dr. Peter Zinterhof
- ♡ Florent Dufour
- ♡ Dr. Naweiluo Zhou
- ♡ Vinzent Bode
- ♡ Dr. Roland Pichler
- ♡ Valentin Pfeil

DigiMed

- ♡ Dr. Jens Wiehler
- ♡ Anja Kroke
- ♡ Ruoyu Sun*
- ♡ Johann Hawe*
- ♡ All partners

Florent AT lrz.de

digimed-admins AT lists.lrz.de